Safety Plan Lane Assistance

Document Version: 1.0

Template Version 2.0, Released on 2017-10-17

Document History

Date	Version	Editor	Description
2017-10-16	1.0	Daniel Gattringer	Initial version

Table of Contents

1. Introduction

1.1. Purpose of the Safety Plan

A Functional Safety Management (FSM) Plan is a key document in any ISO 26262 development project. It specifies how functional safety will be ensured throughout the entire development project and in production.

The safety plan defines the overall framework for a functional safety project in the manner how to handle potential malfunctions of a system according to ISO 26262. ISO 26262 only covers the functional safety of electrical and electronic systems.

The safety plan identifies the various roles and responsibilities as they are applied to the development process. The safety plan lists the various techniques and measures that will be implemented as part of the development project to ensure that the targeted ASIL which is achieved.

1.2. Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

- Concept Phase
- Product Development at the System Level
- Product Development at the Software Level

The following phases are out of scope:

- Product Development at the Hardware Level
- Production and Operation

1.3. Deliverables of the Project

The deliverables of the project are:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

2. Item Definition

2.1. Advanced Driver Assistance System (ADAS)

An Advanced Driver Assistance System has to be developed. Generally spoken an ADAS has the following main functions:

- Alert the driver to potentially dangerous situations
- Take control over the vehicle to prevent accidents from occurring

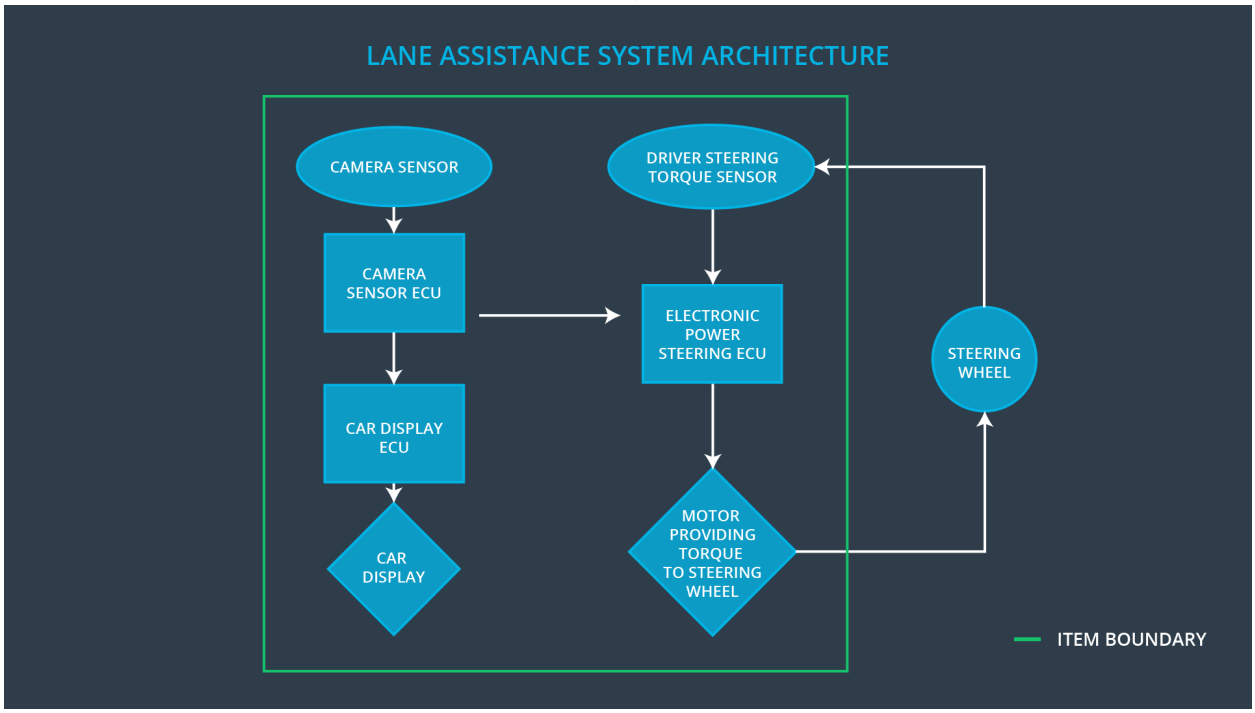
ADAS typically use LIDAR, RADAR and cameras in combination with computer vision technics and deep learning algorithms to get information about the surrounding. ADAS can actually take over control from the driver. Because of this, Functional Safety is a really important issue to consider.

2.2. Lane Assistance System

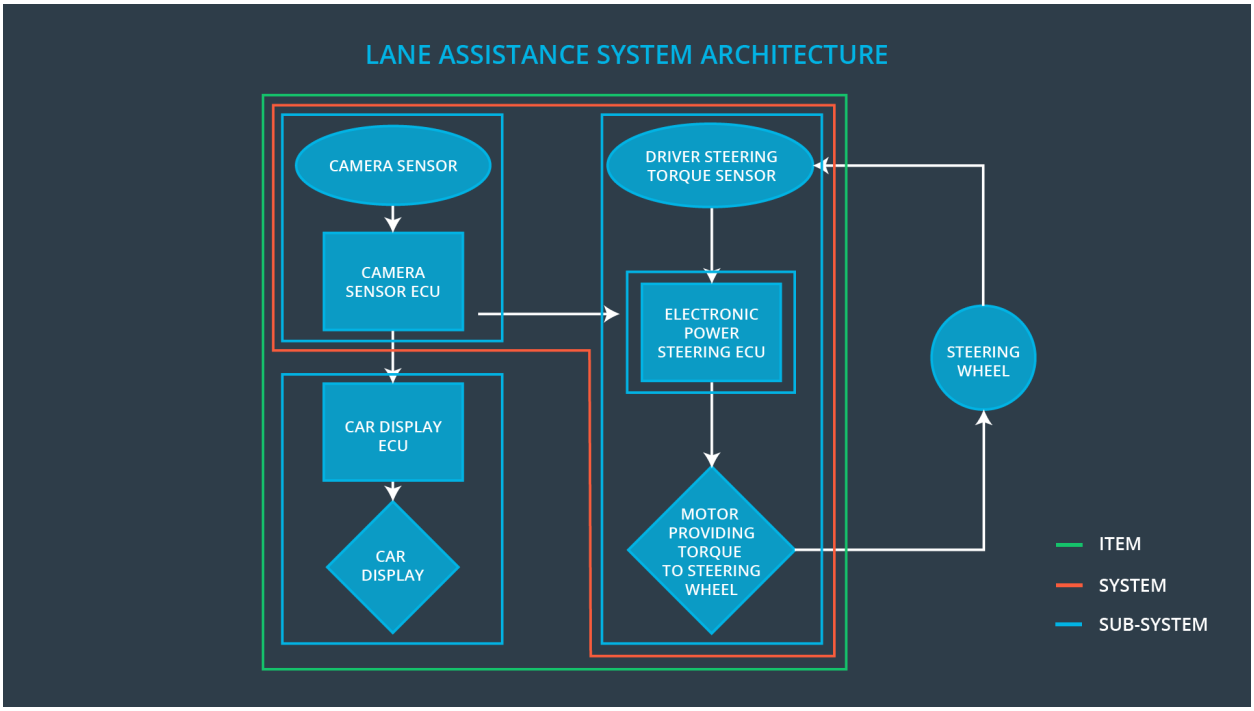
For this project, a simplified version of a Lane Assistance System is analysed. The Lane Assistance System has the following functionalities:

- Lane Departure Warning
- Lane keeping assistance

The item in question is visualized by the following picture:



The item in question can be split up in the following systems/sub-systems:



Sub-System Camera

The camera system detects lane departures and tells the electronic power steering sub-system how hard to turn. The camera system also tells the car display sub-system to display a warning signal when the lane keeping assistance is active.

Sub-System Car Display

The car display visualizes the warning when the lane keeping assistance is active.

Sub-System Electronic Power Steering

The electronic power steering sub-system measures the drivers actual steering torque and receives information about leaving the actual lane from the camera sub-system. The electronic power steering sub-system generates an oscillating steering torque to give the driver a haptic feedback when he/she leaves the actual lane. In addition to this it adds extra steering torque to help the driver move backwards to the centre of the lane.

2.3. Lane Assistance System Functionality

Lane Departure Warning (LDW)

When the driver drifts towards the edge of the lane, the lane departure warning will vibrate the steering wheel. The driver gets warned through this haptic feedback.

Lane Keeping Assistance (LKA)

When the driver drifts towards the edge of the lane, the lane keeping assistance provides automatic assistance to the driver by turning the steering wheel towards the centre of the lane. An activated warning light in the car display dashboard indicates when the lane assistance system is active. If the driver wants to change lane he/she has to use the turn signal which deactivates the lane keeping assistance system. The driver can also turn off the system completely by pressing a button on the dashboard. The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards the centre of the lane. The extra torque is applied directly to the steering wheel via a motor.

The simplified Advanced Driver Assistance (ADAS) does NOT cover functionalities like:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Lane Departure Warning
- Lane Keeping Assistance
- Tire Pressure Monitoring
- Pedestrian Protection

3. Goals and Measures

3.1. Goals

It has to be ensured that the lane assistance system is working in a safe way and never creates harm for the peoples in the vehicle. This includes both functionalities of the system. Therefor methods mentioned in ISO 26262 are used.

The concrete goals of the Lane Assistance Functional Safety Plan are:

- Collect risky situations for the electrical and electronic parts of a tracking system, which can lead to physical damage to vehicle occupants.
- Analyse the risk level of situations.
- Use system engineering methods to reduce the risk to an acceptable level.

3.2. Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All Team Members	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly
Allocate resources with adequate functional safety competency	Project Manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Perform regular functional safety audits	Safety Auditor	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

4. Safety Culture

Technology malfunctions are not the only source of vehicle accidents. Social and organizational factors have to be consider too when a safe systems has to be developed. To do this the organization need clear policies and strategies to support the development, production and operation of the safe systems.

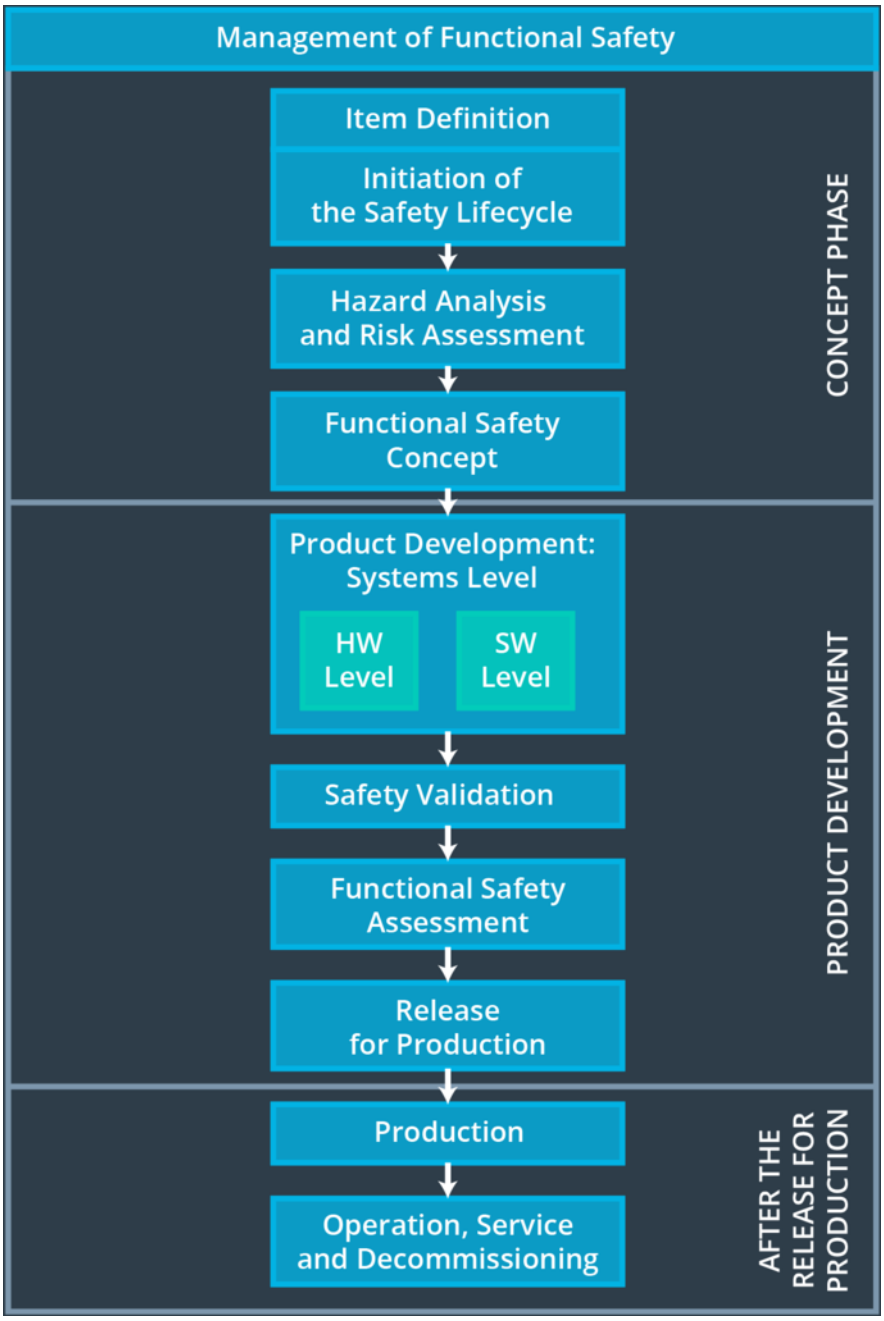
We as an organization rely on the following polies and rules to handle these aspects:

- Quality and Process Management:
  - Fully integrated Quality Management System (ISO 9001).
  - Our behavior is process-driven and all of our processes are well documented and controlled.
- Safety is Prior:
  - Safety has the highest priority over other constraints like cost or productivity.

- Accountability:
    - Our processes ensure that all our design decisions are traceable (time, responsible person, content).
- Resources / Diversity / Communication:
    - Our top management ensures that all of our safety relevant projects are best equipped with people with appropriate skills.
    - Our diverse and highly trained employees ensure that we have all necessary knowledge at our disposal and can consider all topics from different perspectives.
    - Within our communications, we ensure that everything is transparent and that everyone gets the information they need to meet their needs. Employees are encouraged to discuss openly and in a constructive way about possible risks and causes of error and to take a solution-oriented approach.
- Rewards / Penalties:
    - We motivate and support the achievement to reach functional safety.
    - We penalize shortcuts that counteract our safety or quality objectives.

5. Safety Lifecycle Tailoring

The following image shows a flattened version of the used V-model to visualize the while Functional Safety Management Process:



For this functional safety project the ISO 26262 standard process has been tailored to include the following parts of the functional safety lifecycle:

- Concept Phase
- Product Development at the System Level

- Product Development at the Software Level

The following phases are out of scope:

- Product Development at the Hardware Level
- Production and Operation

6. Roles

Role	Org
Functional Safety Manager - Item Level	OEM
Functional Safety Engineer - Item Level	OEM
Project Manager - Item Level	OEM
Functional Safety Manager - Component Level	Tier-1
Functional Safety Engineer - Component Level	Tier-1
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

7. Development Interface Agreement (DIA)

All stakeholders involved in the Lane Assistance Project agree and undertake to comply with the plans contained in this document in order to ensure that the development results are functionally safe in the sense of ISO 26262.

This chapter of the document regulates the cooperation between the OEM *FutureCars* (referred as OEM) and the Tier-1-Supplier *BestComponents* (referred as Tier-1-Supplier). The persons responsible for the implementation of the project are employees of the Tier-1-Supplier. This applies in particular to the two roles *Functional Safety Manager* and *Functional Safety Engineer*.

This chapter ensures to:

- Avoid disputes during the planning and development of the product.
- Regulates liability for possible consequences, damages and hazards.
- Provide clarity which company is best positioned to fix the system if a vehicle has a safety issue after being sold to customers.

OEM responsibilities:

The OEM is supplying a functioning lane assistance system.

Tier-1-responsibilities:

The Tier-1-Supplier analyzes and modifies the various sub-systems to handle functional safety aspects.

8. Confirmation Measures

Confirmation measures ensure that:

- The Lane Assistance Safety Project fulfills the requirements of ISO 26262 (in its tailor-made content).
- The project execution is following the Safety Plan.
- The Lane Assistance Safety Project increases the safety of the vehicle.

The persons who carry out confirmation measures must be independent of the persons who have actually implemented the project.

Confirmation measures:

- Confirmation Review
    - Ensure that the project meets the requirements of ISO 26262.
- Functional Safety Audit
    - Verify that the actual implementation of the project is consistent with the Functional Safety Plan.
- Functional Safety Assessment
    - Confirm that the project increases the functional safety of the vehicle.
    - Confirm that the remaining risks are below the acceptable level.
    - The Assessment includes plans, designs and developed products.